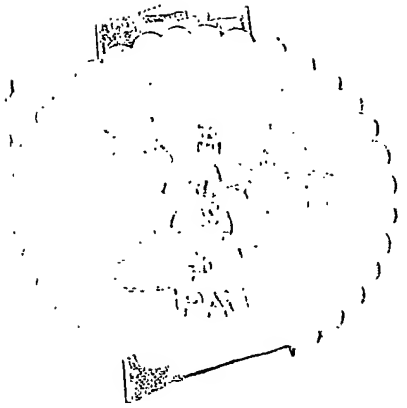
PCT/JP2004/013742
01.10.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年１０月３１日
出願番号 Application Number:	特願２００３－３７３０９７
[ST. 10/C]:	[ＪＰ２００３－３７３０９７]
出願人 Applicant(s):	パイオニア株式会社



２００４年　７月　２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願
【整理番号】　58P0440
【あて先】　特許庁長官　殿
【国際特許分類】　H04L　9/06
　　G09C　1/00　610
【発明者】
　【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内
　【氏名】　多田　謙一郎
【特許出願人】
　【識別番号】　000005016
　【氏名又は名称】　パイオニア株式会社
【代理人】
　【識別番号】　100083839
　【弁理士】
　【氏名又は名称】　石川　泰男
　【電話番号】　03-5443-8461
【手数料の表示】
　【予納台帳番号】　007191
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9102133

【書類名】特許請求の範囲
【請求項１】
少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位と異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、
前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更情報記録領域と、
を備えることを特徴とする情報記録媒体。
【請求項２】
請求項１に記載の情報記録媒体において、
前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報記録媒体。
【請求項３】
請求項１または２に記載の情報記録媒体において、
前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報記録媒体。
【請求項４】
請求項１乃至３のいずれか一項に記載の情報記録媒体において、
前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報記録媒体。
【請求項５】
請求項１乃至４のいずれか一項に記載の情報記録媒体において、
前記画像情報単位は、ＭＰＥＧ（Moving Picture Experts Group）－２ＴＳ（Transport Stream）のシーケンスヘッダと、前記シーケンスヘッダに後続して送信されるＧＯＰ(Group Of Picture)データにより構成されていることを特徴とする情報記録媒体。
【請求項６】
少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報を生成する第１生成手段と、
前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成手段と、
を備えることを特徴とする情報記録装置。
【請求項７】
請求項６に記載の情報記録装置において、
前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報記録装置。
【請求項８】
請求項６または７に記載の情報記録装置において、
前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報記録装置。
【請求項９】
請求項６乃至８のいずれか一項に記載の情報記録装置において、
前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報記録装置。
【請求項１０】
請求項６乃至９のいずれか一項に記載の情報記録装置において、
前記画像情報単位は、ＭＰＥＧ（Moving Picture Experts Group）－２ＴＳ（Transport Stream）のシーケンスヘッダと、前記シーケンスヘッダに後続して送信されるＧＯＰ(Group Of Picture)データにより構成されていることを特徴とする情報記録装置。
【請求項１１】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置であって、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段と、

前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段と、

検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段と、

解読した前記暗号化情報を再生する再生手段と、

を備えることを特徴とする情報再生装置。

【請求項１２】

請求項１１に記載の情報再生装置において、

前記鍵変更情報記録領域は、前記画像単位毎に設けられていることを特徴とする情報再生装置。

【請求項１３】

請求項１１または１２に記載の情報再生装置において、

前記静止画像情報は、フレーム内符号化画像情報であることを特徴とする情報再生装置。

【請求項１４】

請求項１１乃至１３のいずれか一項に記載の情報再生装置において、

前記画像情報単位は、少なくとも一の前記フレーム内符号化画像情報を含む符号化画像情報群により構成されていることを特徴とする情報再生装置。

【請求項１５】

請求項１１乃至１４のいずれか一項に記載の情報再生装置において、

前記画像情報単位は、ＭＰＥＧ（Moving Picture Experts Group）－２ＴＳ（Transport Stream）のシーケンスヘッダと、前記シーケンスヘッダに後続して送信されるＧＯＰ(Group Of Picture)データにより構成されていることを特徴とする情報再生装置。

【請求項１６】

請求項１１乃至１５のいずれか一項に記載の情報再生装置において、

前記解読手段は、検出された前記鍵変更情報が、暗号化された一の前記静止画像情報を解読する処理において二以上の前記暗号鍵が必要であることを示す場合は、当該静止画像情報の解読に必要な暗号鍵を検索する検索手段を備えることを特徴とする情報再生装置。

【請求項１７】

少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第１生成工程と、

前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成工程と、

を備えることを特徴とする情報記録方法。

【請求項１８】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生方法であって、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出工程と、

前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出工程と、

検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読工程と、

解読した前記暗号化情報を再生する再生工程と、

を備えることを特徴とする情報再生方法。

【請求項１９】

少なくとも一の画像情報単位により構成される記録情報を情報記録媒体に記録する情報記録装置に含まれる記録コンピュータを、

前記記録情報を前記画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第１生成手段、

前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成手段、

として機能させることを特徴とする情報記録用プログラム。

【請求項２０】

少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置に含まれる再生コンピュータを、

前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段、

前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段、

検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段、

解読した前記暗号化情報を再生する再生手段、

として機能させることを特徴とする情報再生用プログラム。

【請求項２１】

請求項１９に記載の情報記録用プログラムが前記記録コンピュータで読取可能に記録されていることを特徴とするプログラム記録媒体。

【請求項２２】

請求項２０に記載の情報再生用プログラムが前記再生コンピュータで読取可能に記録されていることを特徴とするプログラム記録媒体。

【書類名】明細書
【発明の名称】情報記録装置及び情報記録方法、情報再生装置及び情報再生方法、情報記録用プログラム、情報再生用プログラム、情報記録媒体並びに記録媒体
【技術分野】
【０００１】
本願は、情報記録装置及び情報記録方法、情報再生装置及び情報再生方法、情報記録用プログラム、情報再生用プログラム、情報記録媒体並びに記録媒体の技術分野に属し、より詳細には、映画等の動画像情報を構成する静止画情報を少なくとも含む記録情報を暗号化して情報記録媒体に記録する情報記録装置及び情報記録方法、当該暗号化して記録されている記録情報を当該情報記録媒体から再生する情報再生装置及び情報再生方法、当該情報記録に用いられる情報記録用プログラム、当該情報再生に用いられる情報再生用プログラム、当該記録情報が記録されている情報記録媒体並びに当該情報記録用プログラム又は情報再生用プログラムが記録された記録媒体の技術分野に属する。
【背景技術】
【０００２】
従来、例えば放送電波を受信して得られたデジタル化された動画像情報をブロック単位で暗号化して記録する装置として、下記特許文献１に開示された暗号化装置がある。かかる暗号化装置は、暗号化に用いられる暗号化鍵を上記ブロック毎に変更するものであって、先ず入力された動画像情報をブロック分割手段で第１のブロックと第２のブロックとに分割し、上記第１のブロックを第１の暗号化手段が第２の中間データを用いて暗号化し、その暗号化結果である第１の暗号化データを出力する。
【０００３】
次に、第２の暗号化手段が、第１の中間データを用い、上記第２のブロックを暗号化し、その暗号化結果である第２の暗号化データを出力する。
【０００４】
その後、ブロック結合手段により、上記出力された第１の暗号化データと第２の暗号化データを結合し、元の動画像情報を暗号化した暗号化情報として出力する構成となっている。
【特許文献１】特開２０００－２６１４２３
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、暗号化されて記録された例えばＭＰＥＧ（Moving Picture Expert Group）トランスポートストリーム（以下、適宜ＴＳ（Transport Stream）と称する）等のデジタル情報を上記特許文献１に開示された発明を用いて再生する場合を考えると、上記ＭＰＥＧトランスポートストリームにおける最小のアクセス単位であるＧＯＰ（Group Of Picture）と同一の暗号化鍵を用いて暗号化される情報単位とが相違していることに起因して、暗号化された同一のＧＯＰ内の例えばＩ（Intra-coded）ピクチャを再生する際に複数の異なる復号化鍵が用いられる形態で当該ＭＰＥＧトランスポートストリームが記録されている場合においては、例えば早送り再生時や再生位置のサーチ時等に、当該Ｉピクチャに対する各暗号化鍵の適用範囲の算出処理を複数の暗号化鍵について再生処理と並行して実行しなければならないこととなり、結果として円滑な再生処理に支障を来たす場合があった。
【０００６】
すなわち、上記特許文献１の発明等を用いる暗号化の場合、その暗号化鍵の適用範囲はいわゆるＣＢＣ（Cipher Block Chain:暗号ブロック連鎖方式）方式の暗号化における暗号化単位であるＣＢＣブロックの数を用いて管理されている場合が多いのに対し、ＭＰＥＧトランスポートストリームのデータの記録態様は、その情報量（バイト数又はパケット数）を基準として管理されており、結果として上記暗号化鍵が適用される範囲と上記ＭＰＥＧトランスポートストリームのデータとの間を関係付ける情報は従来から存在していな

い。

【０００７】

したがって、暗号化鍵の適用範囲（換言すれば、適用切り替わり時点）を算出するには、上記ＭＰＥＧトランスポートストリームのデータを読みながら、その管理ファイル内に記述されている管理情報に基づいて逐一その適用範囲を割り出していかなければならず、上述した早送り再生時や再生位置のサーチ時等の特殊再生時における処理遅延等の支障の原因になると共に、ハードウェア的に見ても処理負荷が大きく、且つその再生処理用のメモリにおける記憶容量を大きくせざるを得ないという問題等が一例として挙げられる。

【０００８】

そこで、本願は、上記の各事情を考慮して為されたもので、その課題の一例は、暗号化鍵の適用範囲（適用切り替わり時点）を逐一算出する必要をなくし、円滑な再生処理及び記録処理等を実現することが可能な情報記録装置及び情報記録方法、当該記録された情報を再生する情報再生装置及び情報再生方法、当該記録に用いられる情報記録用プログラム、当該再生に用いられる情報再生用プログラム、当該情報が記録されている情報記録媒体並びに当該情報記録用プログラム又は情報再生用プログラムが記録された記録媒体の技術分野を提供することにある。

【課題を解決するための手段】

【０００９】

上記の課題を解決するため、請求項１に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位と異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更情報記録領域と、を備える。

【００１０】

上記の課題を解決するために、請求項６に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第１生成手段と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成手段と、を備える。

【００１１】

上記の課題を解決するために、請求項１１に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置であって、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段と、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段と、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段と、解読した前記暗号化情報を再生する再生手段と、を備える。

【００１２】

上記の課題を解決するために、請求項１７に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第１生成工程と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成工程と、を備える。

【００１３】

上記の課題を解決するために、請求項１８に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗

号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生方法であって、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出工程と、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出工程と、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読工程と、解読した前記暗号化情報を再生する再生工程と、を備える。

【００１４】

上記の課題を解決するために、請求項１９に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を情報記録媒体に記録する情報記録装置に含まれる記録コンピュータを、前記記録情報を前記画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更した暗号化情報を生成する第１生成手段、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録する第２生成手段、として機能させる。

【００１５】

上記の課題を解決するために、請求項２０に記載の発明は、少なくとも一の画像情報単位により構成される記録情報を、当該画像情報単位とは異なる暗号化単位の境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されている暗号化情報記録領域と、前記暗号化情報における前記画像情報単位に含まれる静止画像情報の解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録される鍵変更情報記録領域と、が記録されている情報記録媒体から前記記録情報を再生する情報再生装置に含まれる再生コンピュータを、前記情報記録媒体から前記暗号化情報を検出する暗号化情報検出手段、前記情報記録媒体から前記鍵変更情報を検出する鍵変更情報検出手段、検出された前記鍵変更情報に基づいて前記暗号化情報を解読する解読手段、解読した前記暗号化情報を再生する再生手段、として機能させる。

【００１６】

上記の課題を解決するために、請求項２１に記載の発明は、請求項１９に記載の情報記録用プログラムが前記記録コンピュータで読取可能に記録されている。

【００１７】

上記の課題を解決するために、請求項２２に記載の発明は、請求項２０に記載の情報再生用プログラムが前記再生コンピュータで読取可能に記録されている。

【発明を実施するための最良の形態】

【００１８】

以下、本願の実施の形態について、図面を参照しながら説明する。

【００１９】

なお、以下に説明する実施の形態は、ＢＳ(Broadcasting Satellite)デジタル放送に代表されるようなデジタル放送にて配信されるＡＶ(Audio Visual)情報を上記ＣＢＣ方式に則って暗号化した上でハードディスク等の情報記録媒体に記録することが可能とされている情報記録装置、及び上記ＡＶ情報の再生処理が可能とされている情報再生装置に対して夫々本願を適用した場合の実施の形態である。なお、以下の説明では、後述のハードディスク１を共通として一つの筐体に収められている情報記録装置と情報再生装置とを別個に説明する。

【００２０】

また、以下の説明において、上記ＡＶ情報は、動画像の圧縮技術に関する規格として周知のＭＰＥＧ２規格におけるトランスポートストリーム規格に則って放送されてくるものとする。

【００２１】

さらに、以下に説明する記録処理及び再生処理においては、上記暗号化単位としてのＣＢＣブロックに適用される規格、ハードディスクや記録メディアの物理的なアクセス単位に適用される規格、及び上記アクセス単位の情報記録媒体上におけるアクセス開始位置と上記ＣＢＣブロックの当該情報記録媒体上の先頭位置とを合致させることに関する規格は基本的に最低限遵守されるものとする。

【００２２】
上記各規格についてより具体的には、記録されているＡＶ情報に含まれている各コンテンツに対するアクセスは、そのアクセス位置を含むハードディスク等におけるセクタの先頭から行われるものとされている。
【００２３】
また、例えばハードディスク等の物理的なアクセス単位の情報量が５１２バイトであって、論理的にその倍数、例えば６１４４（１２倍）バイト毎にしかアクセスしない場合には、ＣＢＣブロックの情報量をそのアクセス単位の情報量に合わせることになる。すなわち、ハードディスク等におけるアクセス位置とＣＢＣブロックの開始位置とが一致しているものとする。
【００２４】
（Ｉ）記録フォーマットの実施の形態
始めに、本実施の形態に係る情報記録装置について具体的に説明する前に、当該情報記録装置により上記ハードディスクに対して上記ＡＶ情報を記録する際に用いられる論理的な記録フォーマットの概要について、図１及び図２を用いて説明する。
【００２５】
なお、図１及び図２に示す記録フォーマットは、上記ＡＶ情報が当該記録フォーマットに基づいてハードディスクに記録された後の当該記録フォーマットを階層的かつ模式的に夫々示す図である。
【００２６】
また、図１及び図２に示す記録フォーマットは、本実施の形態のＡＶ情報をハードディスクに記録する際に用いられる論理的な記録フォーマットであり、当該記録の際に用いられる物理的な記録フォーマットについては、ハードディスクに用いられている周知の物理フォーマットがそのまま用いられる。
【００２７】
まず、記録されているＡＶ情報の内容及び記録態様を効率的に管理すべく当該記録フォーマットにおいて採用されている種々の概念について、その概要を説明する。
【００２８】
第１に、以下の記録フォーマットにおいては、記録されているＡＶ情報を取り扱う際の単位として、ユニットなる概念が用いられている。すなわち、当該ユニットとは、時間的に連続してハードディスクに記録された一のＡＶ情報をいう。例えば、ＡＶ情報がＢＳデジタル放送で放送された場合は、当該ＢＳデジタル放送における一のイベントが一のユニットとなるように定義されている。
【００２９】
第２に、以下の記録フォーマットにおいては、例えばＢＳデジタル放送中において、放送配信者側の意図によってトランスポートストリーム中の映像情報を格納するパケットのパケットＩＤが同一である部分についてディレクトリなる概念が用いられている。すなわち、ディレクトリとは、一のユニット全体またはその一部を特定して、同一のパケットＩＤである区間を表すものである。
【００３０】
そして、第３に、以下の記録フォーマットにおいては、ユニット中において、ＭＰＥＧ２規格で述べられているＧＯＰを搬送している一の分割区間情報を示す、アプリケーションＧＯＰなる概念が用いられている。このアプリケーションＧＯＰは、ＭＰＥＧ－ＴＳのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるＧＯＰデータとからなり、本願の画像情報単位を構成する。また、上記アプリケーションＧＯＰにより構成されるＭＰＥＧ－ＴＳは、本願の記録情報を構成する。さらに、Ｉピクチャは、本願の静止画像情報であるフレーム内符号化画像情報を構成し、ＧＯＰが本願の符号化画像情報群を構成する。
【００３１】
次に、上述した種々の概念に基づいて本実施の形態に係る論理的な記録フォーマットに

ついて説明する。

【００３２】

図１に示すように、必要なＡＶ情報が記録された後のハードディスク１上には、上記したユニットのそれぞれに対応する管理情報であるユニット情報２と、放送されハードディスク１に記録されているＡＶ情報の実態そのものであるＡＶストリーム情報３と、が記録されている。このＡＶストリーム情報３は、本願の暗号化情報記録領域を構成する。

【００３３】

また、上記ユニット情報２は、暗号化情報４と、上記ＡＶストリーム情報３を管理するための管理情報であるストリーム情報５と、から構成されている。

【００３４】

ここで、当該ストリーム情報５は、ユニットの中に含まれるＴＳパケットの数を示すユニットサイズ６（４バイト）と、ユニット中に含まれるアプリケーションＧＯＰの数を示すポインタテーブル数７（４バイト）と、各アプリケーションＧＯＰの情報を示すポインタテーブル８（アプリケーションＧＯＰの数（図１の場合はｍ個）だけ含まれている）と、により構成されている。

【００３５】

次に、上記ポインタテーブル８の細部構成について、図１及び図２を用いて説明する。

【００３６】

図１に示すように、一のポインタテーブル８は、対応するアプリケーションＧＯＰに含まれるパケット数を示すＧＯＰサイズ９（４バイト）と、対応するアプリケーションＧＯＰの最初のパケットから数えてアプリケーションＧＯＰの中にある最初のＩピクチャを包含し終えるパケットまでの数を示す第１参照画像サイズ１０（２バイト）と、上記最初のＩピクチャが記録されている領域において復号の際に暗号化鍵の変更が必要である旨を表す鍵変更フラグ１１（１バイト）と、により構成されている。この鍵変更フラグ１１は、本願の鍵変更情報記録領域を構成し、アプリケーションＧＯＰ毎に設けられている。

【００３７】

ここで、鍵変更フラグ１１は、ＧＯＰのＩピクチャを復号するために複数の暗号化鍵が必要であることを示すフラグであり、当該複数の暗号化鍵が復号に必要である場合にはその値が「１」とされ、一の暗号化鍵のみでそのＩピクチャが復号できる場合又はそもそも復号が必要でない場合にはその値が「０」とされるものである。すなわち、鍵変更フラグ１１は、暗号化して記録したＭＰＥＧ－ＴＳにおけるアプリケーションＧＯＰに含まれるＩピクチャの解読に複数の鍵が必要か否かを示す鍵変更情報が記録されている。

【００３８】

一方、暗号化情報４は、図２に示すように、上記ユニットを復号しながら再生するために必要な、元のユニットの暗号化に関する情報であり、当該ユニットを復号しながら再生するための暗号化鍵の適用範囲数を示す適用数Ｅと、夫々の適用範囲に関する情報である適用範囲情報１２（各暗号化鍵の適用範囲の数だけ含まれている）と、から構成されている。

【００３９】

また、各適用範囲情報１２は、その適用範囲内を実際に復号するために用いられる暗号化鍵Ｋと、対応する暗号化鍵Ｋの適用開始位置を、ＡＶストリーム情報３の先頭からのＣＢＣブロックの数で表した適用開始ＣＢＣ番号１３と、各適用範囲の大きさをＣＢＣブロックの数で示す適用ＣＢＣ数１４と、から構成されている。

【００４０】

（II）情報記録装置の実施の形態

次に、上述した記録フォーマットを前提としてＡＶ情報をハードディスクに記録する情報記録装置の構成及び動作について説明する。

【００４１】

まず、図３を用いて当該情報記録装置の全体構成及び概要動作について説明する。なお、図３において、ＣＰＵ２５は情報記録装置２０内の全ての構成要素をコントロールする

ものの、簡単のため本実施の形態に関係するコントロール部分のみを図示している。

【００４２】

図３に示すように、本実施の形態の情報記録装置２０は、外部にあるテレビジョン装置ＴＶに直接接続されているとともに、デジタル放送がアンテナにより受信される図示しないデジタル放送受信回路に接続されている。

【００４３】

また、情報記録装置２０は、デマルチプレクサ２１と、映像音声データデコーダ２２と、プレイバックモジュール２３と、レコードモジュール２４と、第１生成手段、第２生成手段及ＣＰＵ２５と、メモリ２６と、ＩＤＥコントローラ２７と、バス２８と、情報記録媒体としてのハードディスク（以下、適宜ＨＤと称する）１と、により構成されている。

【００４４】

次に、概要動作について説明する。

【００４５】

先ず、デマルチプレクサ２１は、上記デジタル放送受信回路から入力されたＭＰＥＧ－ＴＳから必要なパケットのみを抽出する。より具体的には、デマルチプレクサ２１は、ＭＰＥＧ－ＴＳの形式で送信されてくるデジタル放送中からデコードすべき映像信号を搬送しているパケットＩＤを指定することによって、そのビデオ信号のパケットを通過させる。同様に、オーディオ信号やその他の付加的なデータ、その他のＣＰＵ２５で用いるデータを搬送しているパケットＩＤが設定されると、そのパケットＩＤにより示されるパケットを抽出する機能をも備えている。このようにＭＰＥＧ－ＴＳ形式で搬送されてきた情報の中から必要なパケットのみを抽出したものをパーシャルＴＳと呼ぶことにする。

【００４６】

次に、映像音声データデコーダ２２は、デマルチプレクサ２１により得られたパーシャルＴＳからＣＰＵ２５によって指定されたパケットＩＤで搬送されている音声及び映像情報をデコードし、また付加的なデータを抽出し、これらを映像データと音声データとして出力する機能を有する。

【００４７】

一方、プレイバックモジュール２３は、ＨＤ１に記録されているパーシャルＴＳを、ＩＤＥコントローラ２７を用いてデマルチプレクサ２１にデータを供給する。

【００４８】

他方、レコードモジュール２４は、パーシャルＴＳを暗号化しながらＩＤＥコントローラ２７を用いてＨＤ１に暗号化ストリームを記録する。

【００４９】

これらの処理と並行して、ＣＰＵ２５は、上記した全ての構成要素を制御する。このとき、揮発性のメモリ２６は、情報記録の際にはＨＤ１のユニット情報２に相当する情報をその中に構築し、一方、情報再生の際には当該ユニット情報２を一時的に記憶する。

【００５０】

また、ＩＤＥコントローラ２７は、ＡＴＡ（ＡＴ Attachment）のコマンドを発行してＨＤ１とデータ授受を行う。

【００５１】

次に、レコードモジュール２４の内部構成を、図４に用いて説明する。

【００５２】

図４に示すように、レコードモジュール２４は、パーシャルＴＳを取得する情報供給部３１と、暗号化ストリームを出力する暗号化部３２と、から構成され、さらに情報供給部３１は、外部から得られた情報を後段の暗号化部３２に供給し、その際、バッファリング等の処理を行う。

【００５３】

また、情報供給部３１は、ＣＰＵ２５からの制御信号に基づいて、それらの動作を開始又は停止する機能を有している。さらに情報供給部３１には、特定の単位情報を識別したか否かの状態（より具体的には、Ｉピクチャの先頭又はそれに類するシーケンスヘッダコ

ード（ＳＨＣ）やＧＯＰヘッダを検出した状態、検出後の別なピクチャの先頭の検出した後の状態等）を保持する特定単位情報識別状態フラグ３１ａが設定されており、その特定単位情報識別状態フラグ３１ａは他の構成部材から参照可能とされている。このとき、情報供給部３１では、特定の単位情報を識別する動作を続けており、常に状態を遷移させている。そして、情報供給部３１は、パケットカウンタ３１ｂをさらに有しており、入力されたパケットをカウントし、そのカウント値を示すデータを保持する。

【００５４】

一方、暗号化部３２は、ＣＢＣブロックの数を計数するＣＢＣカウンタ３２ａを有し、ＣＰＵ２６からの制御信号に基づいて暗号鍵を生成し、情報供給部３１から得られた情報を固定長の暗号ブロック毎に暗号化し、後段の手段に情報を出力する。

【００５５】

なお、記録終了時点では、ＣＰＵ２５がメモリ２６内の情報をユニット情報２としてＨＤ１に書き込む動作を行う。これにより、ＨＤ１内の論理情報が構築される。

【００５６】

（II－Ａ）記録処理

次に、ＣＰＵ２５を中心とした情報記録装置２０による記録処理について、図５を参照して説明する。

【００５７】

ＣＰＵ２５は、ステップＳ１で初期化処理を実行する。すなわち、この初期化処理では、暗号化情報４の適用数Ｅの値を「０」、パケットカウンタ３１ｂの値を「０」、前アプリケーションＧＯＰ位置の値を「０」、ＣＢＣカウンタ３２ａの値を「０」、特定単位情報識別状態フラグ３１ａの値を「０」、アプリケーションＧＯＰ指数の値を「０」、適用範囲情報１２の適用開始ＣＢＣ番号１３の値を「０」に設定する処理を夫々に行う。

【００５８】

次に、暗号化部３２にて暗号鍵を生成して待機し、適用範囲情報１２の鍵Ｋを決定し、暗号化情報４の適用数Ｅをインクリメントした後（ステップＳ２）、情報供給部３１でいずれかのピクチャの検出動作をスタートし、パーシャルＴＳの入力を開始する（ステップＳ３）。

【００５９】

ステップＳ４では、情報供給部３１で最初のシーケンスヘッダコードを検出するまで待機し、最初のシーケンスヘッダコードを検出した場合に特定単位情報識別状態フラグ３１ａの値を「１」とする（ステップＳ５）。

【００６０】

ステップＳ６において、情報供給部３１は、パケットを一つ入力し、パケットカウンタ３１ｂをインクリメントした後、暗号化補助動作を実行する（ステップＳ７）。なお、この暗号化補助動作については後ほど詳述する。

【００６１】

ステップＳ８では、ＣＰＵ２５は、情報供給部３１で次のピクチャが検出されたか否かを判定し、次のピクチャが検出された場合（ステップＳ８；ＹＥＳ）には、ステップＳ９に進み、特定単位情報識別状態フラグ３１ａの値を「０」とする。一方、次のピクチャが検出されない場合（ステップＳ８；ＮＯ）には、ステップＳ６に戻り、次のピクチャが検出されるまで、ステップＳ６及びステップＳ７の処理を繰り返す。

【００６２】

次に、ステップＳ１０では、パケットカウンタ３１ｂの値から前アプリケーションＧＯＰ位置の値を減算し、対応するアプリケーションＧＯＰ内の第１参照画像サイズ１０に格納し、ステップＳ６及びステップＳ７と同様にステップＳ１１でパケットを一つ入力し、パケットカウンタ３１ｂの値をインクリメントした後、上記暗号化補助動作を再度実行する（ステップＳ１２）。

【００６３】

次に、ステップＳ１３において、ＣＰＵ２５は、シーケンスヘッダコードが検出された

か否かを判定し、当該シーケンスヘッダコードが検出された場合（ステップＳ１３；ＹＥＳ）には、ステップＳ１４に進み、パケットカウンタ３１ｂの値から前アプリケーションＧＯＰ位置の値を減算して対応するアプリケーションＧＯＰ内のＧＯＰサイズ９に格納する。一方、シーケンスヘッダコードが検出されない場合（ステップＳ１３；ＮＯ）には、ステップＳ１１に戻り、シーケンスヘッダコードが検出されるまで、ステップＳ１１及びステップＳ１２の処理を繰り返す。

【００６４】

これにより、ステップＳ１５では、アプリケーションＧＯＰの番号を示すパラメータｉをインクリメントした後、パケットカウンタ３１ｂの値を前アプリケーションＧＯＰ位置の値に格納する（ステップＳ１６）。そして、ステップＳ５に戻り、当該ステップＳ５以下の処理を繰り返す。

【００６５】

（II－Ｂ）暗号化補助動作処理

次に、ＣＰＵ２５による上記暗号化補助動作処理の詳細について、図６を用いて説明する。

【００６６】

当該暗号化補助動作処理において、ＣＰＵ２５は、先ずステップＳ２１で特定単位情報識別状態フラグ３１ａが「１」であるか否かを判定し、特定単位情報識別状態フラグ３１ａの値が「１」である場合（ステップＳ２１；ＹＥＳ）には、ステップＳ２２で新しい暗号鍵が生成されたか否か次に判定する。そして、新しい暗号鍵が生成された場合（ステップＳ２２；ＹＥＳ）には、一つ前（Ｅ－1番目）の適用範囲情報１２内の適用ＣＢＣ数１４の値を、そのときのＣＢＣカウンタ３２ａの値から当該一つ前（Ｅ－1番目）の適用範囲情報１２内の適用開始ＣＢＣ番号１３の値を減算した値とし（ステップＳ２３）、さらに、Ｅ番目の適用範囲情報１２内の適用開始ＣＢＣ番号１３の値を、そのときのＣＢＣカウンタ３２ａの値とし（ステップＳ２４）、その後に適用数Ｅをインクリメントする（ステップＳ２５）。

【００６７】

ステップＳ２６では、図示しない暗号化バッファ内にデータがあるか否かを判定し、データがある場合（ステップＳ２６；ＹＥＳ）には、ステップＳ２７でｉ番目のアプリケーションＧＯＰにおける鍵変更フラグ１１の値を「１」とした後、ステップＳ２８に進む。

【００６８】

なお、ステップＳ２１で特定単位情報識別状態フラグ３１ａの値が「１」でない場合（ステップＳ２１；ＮＯ）、ステップＳ２２で新しい暗号鍵が生成されない場合（ステップＳ２２；ＮＯ）及びステップＳ２６で暗号化バッファ内にデータがない場合（ステップＳ２６；ＮＯ）には、それぞれ直接ステップＳ２８に進む。

【００６９】

そして、ステップＳ２８では、暗号化バッファ内のデータの情報量が一のＣＢＣブロックの情報量に到達したか否かを判定し、そのデータの情報量が一ＣＢＣブロックの情報量に達した場合（ステップＳ２８；ＹＥＳ）には、ステップＳ２９において対応するＣＢＣ単位で暗号化した後、ＣＢＣカウンタ３２ａをインクリメントして暗号化後の情報を記録する（ステップＳ３０、Ｓ３１）。

【００７０】

なお、ステップＳ２８で、蓄積されているデータ量が、ＣＢＣブロックの情報量に達していない場合（ステップＳ２８；ＮＯ）には、ステップＳ２１に戻る。これら一連の処理を実行することにより、暗号化補助動作を終了する。

【００７１】

（II－Ｃ）ＲＡＭに展開された記録フォーマットの実施の形態

次に、本実施の形態において、図３に示すメモリ２６がＲＡＭであって、当該メモリ２６に展開されたストリーム情報５を図７を用いて、メモリ２６に展開された暗号化情報４を図８を用いて、夫々説明する。なお、図７及び図８において、図１及び図２と同一の部

分には、同一の符号を付してその説明を省略する。

【００７２】

本実施の形態では、記録処理を実行する際、メモリ２６内に必要なユニット情報２が展開されつつ構築される。

【００７３】

すなわち、メモリ２６内に設定されるストリーム情報一時記憶領域３６に展開されたストリーム情報５は、図７に示すように、図１と同様にユニットの中に含まれるＴＳパケットの数を示すユニットサイズ６と、ユニット中に含まれるアプリケーションＧＯＰの数を示すポインタテーブル数７と、アプリケーションＧＯＰの情報を示すポインタテーブル８と、により構成されている。

【００７４】

また、同じくメモリ２６内に設定される暗号化情報一時記憶領域３５に展開された暗号化情報４は、図８に示すように、図２と同様の適用数Ｅと、夫々の適用範囲に関する情報である適用範囲情報１２と、から構成されている。

【００７５】

（II－Ｄ）記録終了処理

次に、ＣＰＵ２５を中心としてＨＤ１への一連の記録処理を終了する際に実行される記録終了処理について、図９を用いて説明する。

【００７６】

当該記録終了処理においては、先ず、ＣＰＵ２５は、暗号化情報一時記憶領域３５から暗号化情報４を、ストリーム情報一時記憶領域３６からストリーム情報５を、夫々読み出してユニット情報２として記録し（ステップＳ３５）、全ての記録動作を終了する（ステップＳ３６）。

【００７７】

（III）情報再生装置の実施の形態

次に、上述した記録フォーマットを用いてＨＤ１に記録されているＡＶストリーム情報３を再生する情報再生装置の構成及び動作について説明する。

【００７８】

まず、図１０を用いて当該情報再生装置の全体構成及び概要動作について説明する。

【００７９】

図１０に示すように、本実施の形態の情報再生装置４０は、情報出力部４１と、鍵変更情報検出手段、解読手段及び検索手段としての非暗号化部４２と、暗号化情報検出手段及び再生手段としての読出し部４３とから構成されている。非暗号化部４２は、検出された鍵変更情報が、暗号化されたＩピクチャを解読する処理において二以上の鍵Ｋが必要であることを示す場合は、当該Ｉピクチャの解読に必要な鍵Ｋを検索する。また、読出し部４３は、上記ＨＤ１から得られた暗号化された情報（暗号化されたパーシャルＴＳ）を非暗号化部４２に出力する。

【００８０】

これにより、非暗号化部４２は、図示しないＣＰＵからの制御によって読出し部４３から得られたパーシャルＴＳを上記ＣＢＣブロック毎に解読し、情報出力部４１に復号されたパーシャルＴＳとして出力する。

【００８１】

そして、情報出力部４１は、非暗号化部４２から得られた復号後のパーシャルＴＳを、予め設定されたバッファ処理等を実行しつつ外部に供給する。また、情報出力部４１は、図示しないＣＰＵからの制御によって、それらの動作を開始及び停止する機能を有している。

【００８２】

（III－Ａ）通常再生処理

次に、図示しないＣＰＵによる通常再生処理について、図１１を用いて説明する。なお、当該再生処理は、ＨＤ１に記録されているＡＶストリーム情報３の先頭から通常再生す

る処理である。

【００８３】

まず、ステップＳ４１で情報取得アドレスを「０」にした後、再生処理を中止する操作が図示しない操作部において実行されたか否かを判定し（ステップＳ４２）、その操作が実行された場合（ステップＳ４２；ＹＥＳ）には、再生処理を終了する。

【００８４】

一方、再生処理の中止操作が実行されない場合（ステップＳ４２；ＮＯ）には、ステップＳ４３に進み、情報取得アドレスの位置からＡＶストリーム情報３を取得する。

【００８５】

次いで、ステップＳ４４では、情報取得アドレスに相当するＣＢＣブロックの適用範囲を検索し、その検索結果から適用範囲情報１２を取得し、鍵Ｋを得る（ステップＳ４５）。なお、当該ステップＳ４４の処理については、後述する。

【００８６】

そして、ステップＳ４６では、読出し部４３から得られたパーシャルＴＳを非暗号化部４２により固定長のＣＢＣブロック毎に鍵Ｋを用いて復号した後、情報取得アドレスをインクリメントする（ステップＳ４７）。以下、ステップＳ４２で再生が中止されるまでステップＳ４３からステップＳ４７までの処理を繰り返す。

【００８７】

なお、情報取得アドレスに相当する適用範囲を検索するため、図２に示す暗号化情報４内の適用範囲情報１２を順次参照する動作が発生する。但し、図１１に示す通常再生の場合は、情報取得アドレスをＣＢＣブロックの情報量の定数倍としてもよく、このようにＣＢＣブロックの情報量の定数倍とした場合には、ＣＢＣブロックの適用範囲の検索が容易になる。

【００８８】

（III－Ｂ）適用範囲検索処理

次に、上記ステップＳ４４としての適用範囲検索処理について、図１２を用いて詳説する。なお、当該適用範囲検索処理は、ＡＶストリーム情報３内のアクセス位置（ＣＢＣ数）に換算し、現在どの鍵Ｋが必要かを検索するルーチンである。

【００８９】

まず、ステップＳ５１でＡＶストリーム情報３内のアクセス位置（バイト数）ＰをＣＢＣブロックの情報量で除して現在のアクセス位置（ＣＢＣ数）ｐを求めた後、パラメータｉを「１」とする（ステップＳ５２）。ここで、図１２において、パラメータｉはＣＢＣ換算での適用範囲の番号を示すパラメータである。

【００９０】

次いで、ステップＳ５３では、パラメータｉが暗号化情報４の適用数Ｅ未満であるか否かを判定し、パラメータｉが適用数Ｅ未満の場合（ステップＳ５３；ＹＥＳ）には、ステップＳ５４でアクセス位置（ＣＢＣ数）ｐがＣＢＣブロック換算でｉ番目の適用範囲ｘ（ｉ）以上であるかを判定し、適用範囲ｘ（ｉ）以上の場合（ステップＳ５４；ＹＥＳ）には、ステップＳ５５でそのアクセス位置（ＣＢＣ数）ｐが、「適用範囲ｘ（ｉ）＋適用サイズｙ（ｉ）」未満であるかを判定し、「適用範囲ｘ（ｉ）＋適用サイズｙ（ｉ）」未満の場合（ステップＳ５５；ＹＥＳ）には、ステップＳ５６でメインルーチンに戻るときの戻り値を「ｉ」として検索処理を終了する。

【００９１】

一方、ステップＳ５３で適用数Ｅがパラメータｉ以上の場合（ステップＳ５３；ＮＯ）には、ステップＳ５７で戻り値を「１」だけデクリメントして検索処理を終了する。

【００９２】

また、ステップＳ５４で適用範囲ｘ（ｉ）がアクセス位置（ＣＢＣ数）ｐの外である場合（ステップＳ５３；ＮＯ）、及びステップＳ５５で「適用範囲ｘ（ｉ）＋適用サイズｙ（ｉ）」がアクセス位置（ＣＢＣ数）ｐの外である場合（ステップＳ５５；ＮＯ）には、ステップＳ５８でパラメータｉをインクリメントしてステップＳ５３に戻る。

【００９３】
（III－Ｃ）特殊再生処理
（Ｃ－１）第１特殊再生処理
次に、図示しないＣＰＵによる、通常再生以外の特殊再生処理について、図１３を用いて説明する。
【００９４】
なお、図１３に示す特殊再生処理は、鍵変更フラグ１１を参照しながら動作する、早送り再生又は検索処理等の特殊再生ルーチンである。
【００９５】
まず、ステップＳ６１では、最初のディレクトリにおいて最初のポインタテーブルを参照するように初期化する。
【００９６】
ステップＳ６２では、最初のＩピクチャの位置を、「最初のディレクトリのパケットポインタ（バイト）＋ＧＯＰパケットポインタ（パケット数）×パケットサイズ（バイト）」を情報取得アドレスＮ（バイト）として求める。
【００９７】
ステップＳ６２では、特殊再生終了指示があったか否かを判定し、特殊再生終了指示があった場合（ステップＳ６２；ＹＥＳ）には、特殊再生処理を終了する。一方、特殊再生終了指示がない場合（ステップＳ６２；ＮＯ）には、ステップＳ６４に進み、第１参照画像サイズ１０から読込バイト数Ｍを取得した後、情報取得アドレスＮに相当する鍵Ｋの適用範囲を検索する（ステップＳ６５）。
【００９８】
ステップＳ６６では、図示しないＣＰＵは鍵変更フラグ１１が「０」でないかを判定し、鍵変更フラグ１１が「０」でない場合（ステップＳ６６；ＹＥＳ）には、「情報取得アドレスＮ＋読込バイト数Ｍ」の位置にあるデータを復号するための鍵Ｋの適用範囲を検索して復号する（ステップＳ６７，Ｓ６８）。なお、鍵変更フラグ１１が「０」の場合（ステップＳ６６；ＮＯ）には、直接ステップＳ６８に進んで復号する。
【００９９】
ステップＳ６９では、情報取得アドレスＮに「ＧＯＰサイズ（パケット数）×パケットサイズ」を加算して情報取得アドレスＮを変更した後、次のポインタテーブル８を参照するように変更する（ステップＳ７０）。
【０１００】
そして、これ以後、ステップＳ６３で特殊再生終了指示があるまでステップＳ６４からステップＳ７０までの処理を繰り返す。
【０１０１】
（Ｃ－２）第２特殊再生処理
次に、図示しないＣＰＵによる第２特殊再生処理について、図１４を用いて説明する。
【０１０２】
なお、図１４に示す第２特殊再生処理は、適用範囲情報１２の最適化を行って検索ルーチンを省いた特殊再生ルーチンである。また、図１３に示す第１特殊再生処理と同一の処理は、同一のステップ番号を付してその説明を省略する。
【０１０３】
図１４に示す第２特殊再生処理は、ステップＳ６６で鍵変更フラグ１１が「０」でないかを判定し、鍵変更フラグ１１が「０」でない場合（ステップＳ６６；ＹＥＳ）には、ステップＳ６７ａにおいて次の適用範囲情報１２を得るようにしている。
【０１０４】
ここで、仮に上記適用範囲情報１２がアクセスする順に並んでいるとし、且つ適用範囲１２の間に空隙がないとするならば、図１３に示す第１特殊再生処理のように「情報取得アドレスＮ＋読込バイト数Ｍ」からの適用範囲検索を省略し、現在アクセスしている適用範囲情報１２の次の適用範囲情報１２をアクセスするようにしてもよい。

【０１０５】

(IV) 鍵変更フラグの他の実施形態

次に、鍵変更フラグ１１の他の実施形態について、図１５を用いて説明する。なお、図１５は、鍵変更フラグ１１の拡張を示す説明図である。なお、図１５（Ａ）及び（Ｂ）において、ハッチング部分は、鍵Ｋが変更されていることを示している。

【０１０６】

上述した実施形態においては、鍵変更フラグ１１を１バイトの情報として説明したが、これ以外に、鍵変更フラグを、一のアプリケーションＧＯＰ内において鍵Ｋが変更されたか否かを示す前半四ビットの情報と、一のＩピクチャの復号中に鍵Ｋが変更されるか否かを示す後半四ビットの情報とで、構成するように拡張することもできる。

【０１０７】

この場合、前半四ビットの情報につき、値「０００００ｂ（ｂは二進数であることを示す。以下、同様）」は対応するアプリケーションＧＯＰ再生中に鍵Ｋの変更が必要無いことを示し、値「００００１ｂ」は対応するアプリケーションＧＯＰ再生中に鍵Ｋの変更が必要であることを示し、値「００１０ｂ」は対応するアプリケーションＧＯＰ再生中にＡＶストリーム情報３の終了点が存在することを示し、値「００１１ｂ」は対応するアプリケーションＧＯＰ再生中にＡＶストリーム情報３の開始点が存在することを示すものと定義づける。

【０１０８】

一方、後半四ビットの情報につき、値「００００ｂ」は対応するＩピクチャの読み込みに鍵Ｋの変更が必要無いことを示し、値「００００１ｂ」は対応するＩピクチャの読み込みに鍵Ｋの変更が必要であることを示し、値「００１０ｂ」は対応するＩピクチャの途中にＡＶストリーム情報３の終了点が存在することを示し、値「００１１ｂ」は対応するＩピクチャの途中にＡＶストリーム情報３の開始点が存在することを示すものと定義づける。

【０１０９】

このように定義付けて鍵変更フラグを上記実施形態のように用いれば、例えば、図１５（Ａ）に示すようにアプリケーションＧＯＰの途中であって、Ｉピクチャの途中に鍵Ｋの変更位置がある場合は、鍵変更フラグの値を「００００１ｂ－００００１ｂ」として表現できる。

【０１１０】

また、図１５（Ｂ）に示すようにアプリケーションＧＯＰの途中に鍵Ｋの変更位置があるものの、Ｉピクチャの途中には鍵Ｋの変更位置がない場合は、鍵変更フラグの値を「００００１ｂ－００００ｂ」として表現できる。

【０１１１】

さらに、図１５（Ｃ）に示すように、アプリケーションＧＯＰの途中であって、Ｉピクチャの途中から暗号化されていない場合は、鍵変更フラグの値を「００１０ｂ－００１０ｂ」として表現できる。

【０１１２】

最後に、図１５（Ｄ）に示すように、アプリケーションＧＯＰの途中から暗号化されているがＩピクチャは暗号化されていない場合は、鍵変更フラグの値を「００１１ｂ－００００ｂ」として表現できる。

【０１１３】

このように、図１５（Ａ）乃至（Ｄ）に示すように、ＩピクチャだけでなくアプリケーションＧＯＰ中に鍵Ｋの変更位置が存在する場合でも鍵変更フラグを用いて表現することができるのである。

【０１１４】

以上説明したように、本実施の形態のＨＤ１によれば、アプリケーションＧＯＰにより構成されるＭＰＥＧ２規格におけるトランスポートストリームを、当該アプリケーションＧＯＰと異なるＣＢＣブロックの境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されているＡＶストリーム情報３と、上記暗号化情報におけるアプリケー

ションＧＯＰに含まれるＩピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更フラグ１１と、が記録されているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１１５】

また、鍵変更フラグ１１は、アプリケーションＧＯＰ毎に設けられているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１１６】

さらに、静止画像情報としてＩピクチャを解読するので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１１７】

そして、アプリケーションＧＯＰは、ＭＰＥＧ２規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるＧＯＰと、により構成されているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１１８】

本実施の形態の情報記録装置２０によれば、アプリケーションＧＯＰにより構成されるＭＰＥＧ２規格におけるトランスポートストリームを、当該アプリケーションＧＯＰと異なるＣＢＣブロックの境界において暗号鍵を変更した暗号化情報を生成するＣＰＵ２５と、上記暗号化情報におけるアプリケーションＧＯＰに含まれるＩピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報を記録するＣＰＵ２５と、を備えているので、情報記録装置２０において鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１１９】

また、鍵変更フラグ１１は、アプリケーションＧＯＰ毎に設けられているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１２０】

さらに、静止画像情報としてＩピクチャを解読するので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１２１】

そして、アプリケーションＧＯＰは、ＭＰＥＧ２規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるＧＯＰと、により構成されているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。

【０１２２】

さらにまた、本実施の形態の情報再生装置４０によれば、ＨＤ１から暗号化情報を検出する読出し部４３と、ＨＤ１から鍵変更情報を検出する非暗号化部４２と、検出された鍵変更情報に基づいて暗号化情報を解読する非暗号化部４２と、解読した暗号化情報を再生する読出し部４３と、を備えているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さくすることができる。

【０１２３】
また、鍵変更フラグ１１は、アプリケーションＧＯＰ毎に設けられているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。
【０１２４】
さらに、静止画像情報としてＩピクチャを解読するので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。
【０１２５】
そして、アプリケーションＧＯＰは、ＭＰＥＧ２規格におけるトランスポートストリームのシーケンスヘッダと、当該シーケンスヘッダに後続して送信されるＧＯＰと、により構成されているので、鍵Ｋの適用切り替わり時点を逐一算出する必要がなくなり、円滑な処理を実行することができるとともに、ハードウェア的な負荷を小さく、且つメモリ２６の容量を少なくすることができる。
【０１２６】
なお、本願は上記実施の形態に限定されることなく、種々の変更が可能である。
【０１２７】
例えば、上記実施の形態では、ＢＳデジタル放送等の電波を受信して映像信号等を取得するようにしたが、これ以外にアナログ地上波ＴＶ放送の電波や、インターネット又は専用回線を介したサーバＶＯＤ(Video On Demand)から映像信号等を取得するようにしてもよい。
【０１２８】
また、上記実施の形態では、記録媒体としてＨＤ１を用いた場合について説明したが、これ以外に情報の書き換えが可能なＤＶＤやフラッシュメモリ等の各種記録媒体を使用することができる。
【０１２９】
さらに、図５、図６、図９、図１１乃至図１４に示すフローチャートに対応するプログラムを、フレキシブルディスク又はＨＤ等の情報記録媒体に記録させておき、或いは当該プログラムをインターネット等のネットワークを介して取得した後に記録しておき、これらを汎用のマイクロコンピュータ等により読み出して実行することにより、当該マイクロコンピュータを実施の形態に係るＣＰＵ２５等として機能させることが可能である。

【図面の簡単な説明】

【０１３０】
【図１】本実施形態の記録フォーマットのストリーム情報を示す説明図である。
【図２】本実施形態の記録フォーマットの暗号化情報を示す説明図である。
【図３】本実施形態の情報記録装置の全体構成を示すブロック図である。
【図４】レコードモジュールの内部構成を示すブロック図である。
【図５】本実施形態の記録処理を示すフローチャートである。
【図６】本実施形態の暗号化補助動作処理を示すフローチャートである。
【図７】本実施形態においてＲＡＭに展開されたストリーム情報のフォーマットを示す説明図である。
【図８】本実施形態においてＲＡＭに展開された暗号化情報のフォーマットを示す説明図である。
【図９】本実施形態の記録終了処理を示すフローチャートである。
【図１０】本実施形態の情報再生装置を示すブロック図である。
【図１１】本実施形態の再生処理を示すフローチャートである。
【図１２】本実施形態の検索処理を示すフローチャートである。
【図１３】本実施形態の特殊再生処理を示すフローチャートである。
【図１４】本実施形態の他の特殊再生処理を示すフローチャートである。

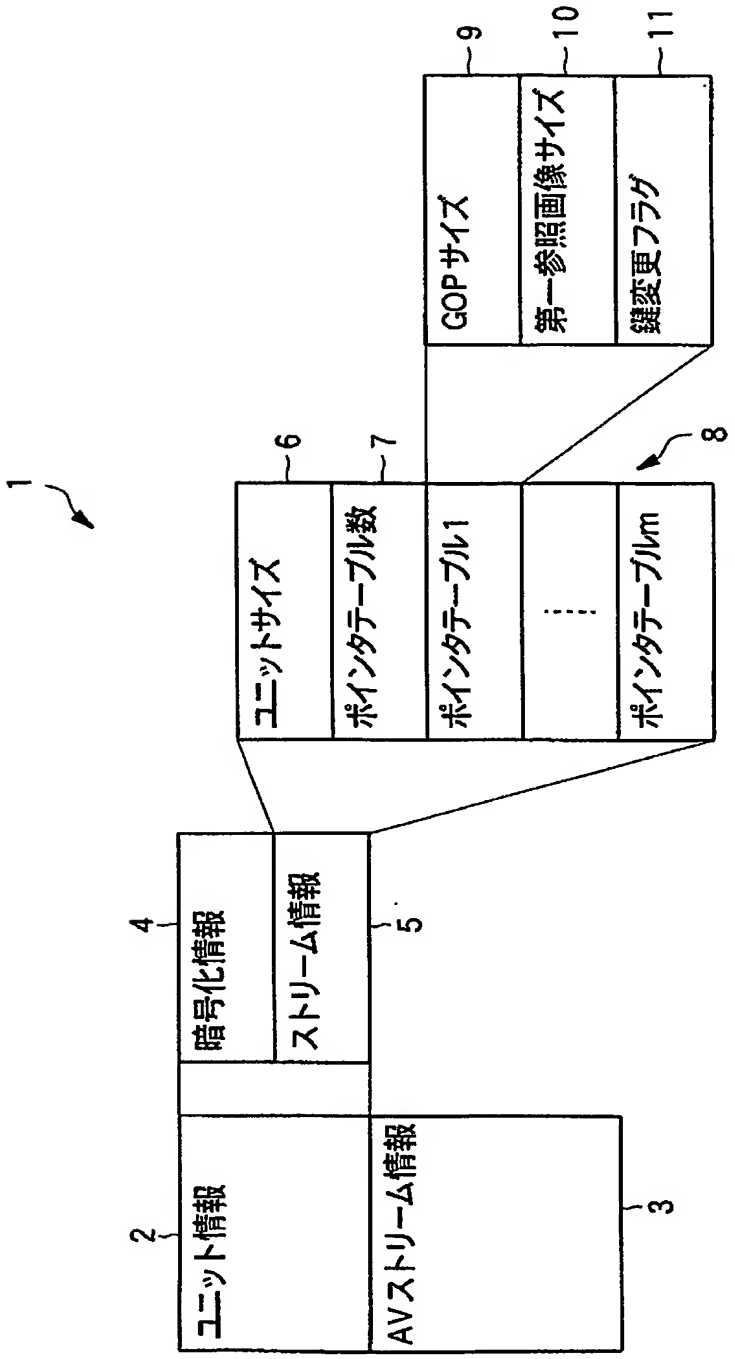
【図１５】本実施形態の鍵変更フラグの拡張態様を示す説明図であり、（Ａ）は第１の例を示す図であり、（Ｂ）は第２の例を示す図であり、（Ｃ）は第３の例を示す図であり、（Ｄ）は第４の例を示す図である。

【符号の説明】

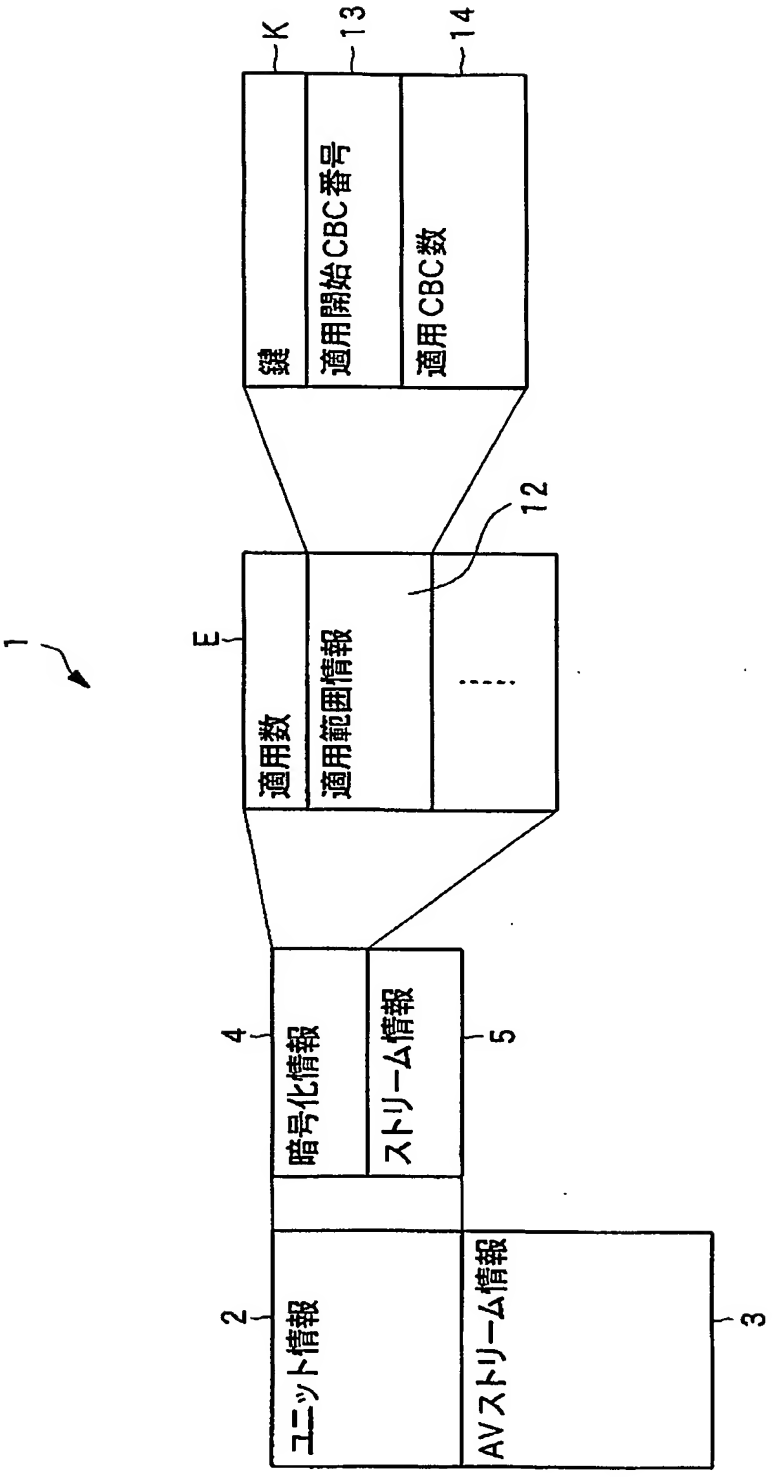
【０１３１】

１　ＨＤ
２　ユニット情報
３　ＡＶストリーム情報
４　暗号化情報
５　ストリーム情報
８　ポインタテーブル
９　ＧＯＰサイズ
１０　第１参照画像サイズ
１１　鍵変更フラグ
１２　適用範囲情報
１３　適用開始ＣＢＣ番号
１４　適用ＣＢＣ数
２０　情報記録装置
２１　デマルチプレクサ
２２　映像、音声データデコーダ
２４　レコードモジュール
２５　ＣＰＵ
２６　メモリ
３１　情報供給部
３２　暗号化部
４０　情報再生装置
４１　情報出力部
４２　非暗号化部
４３　読出し部

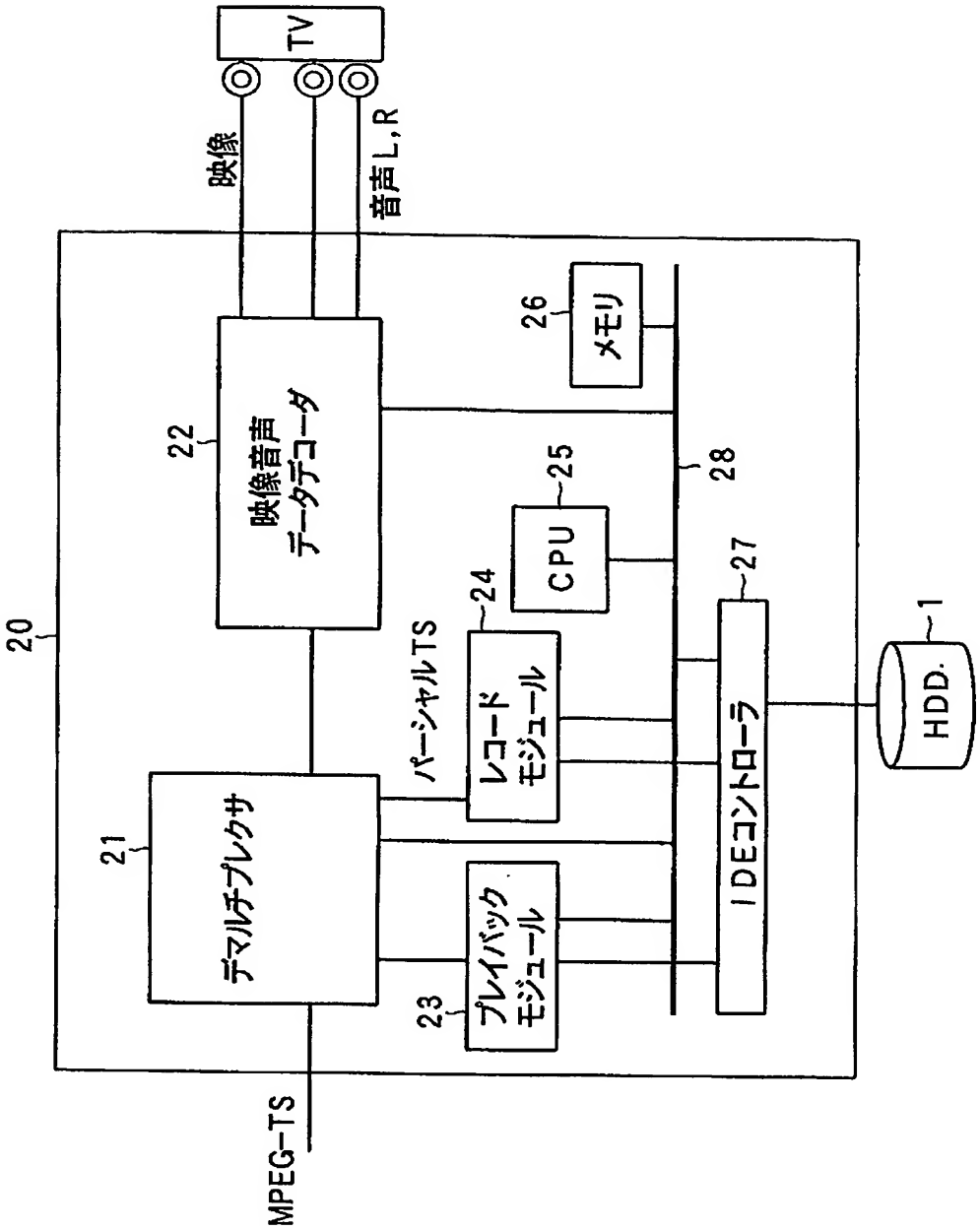
【書類名】図面
【図１】


1
2
ユニット情報
3
AVストリーム情報
4
暗号化情報
5
ストリーム情報
6
ユニットサイズ
7
ポインタテーブル数
8
ポインタテーブル1
ポインタテーブルm
9
GOPサイズ
10
第一参照画像サイズ
11
鍵変更フラグ

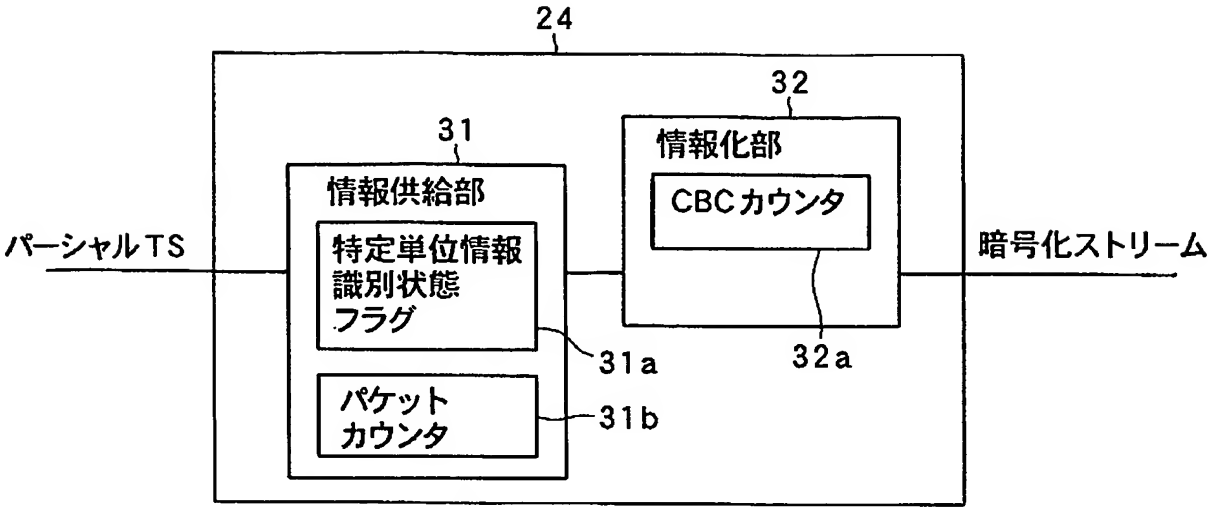
【図２】


1
E
適用数
適用範囲情報
12
K
鍵
13
適用開始CBC番号
14
適用CBC数
4
暗号化情報
5
ストリーム情報
2
ユニット情報
3
AVストリーム情報

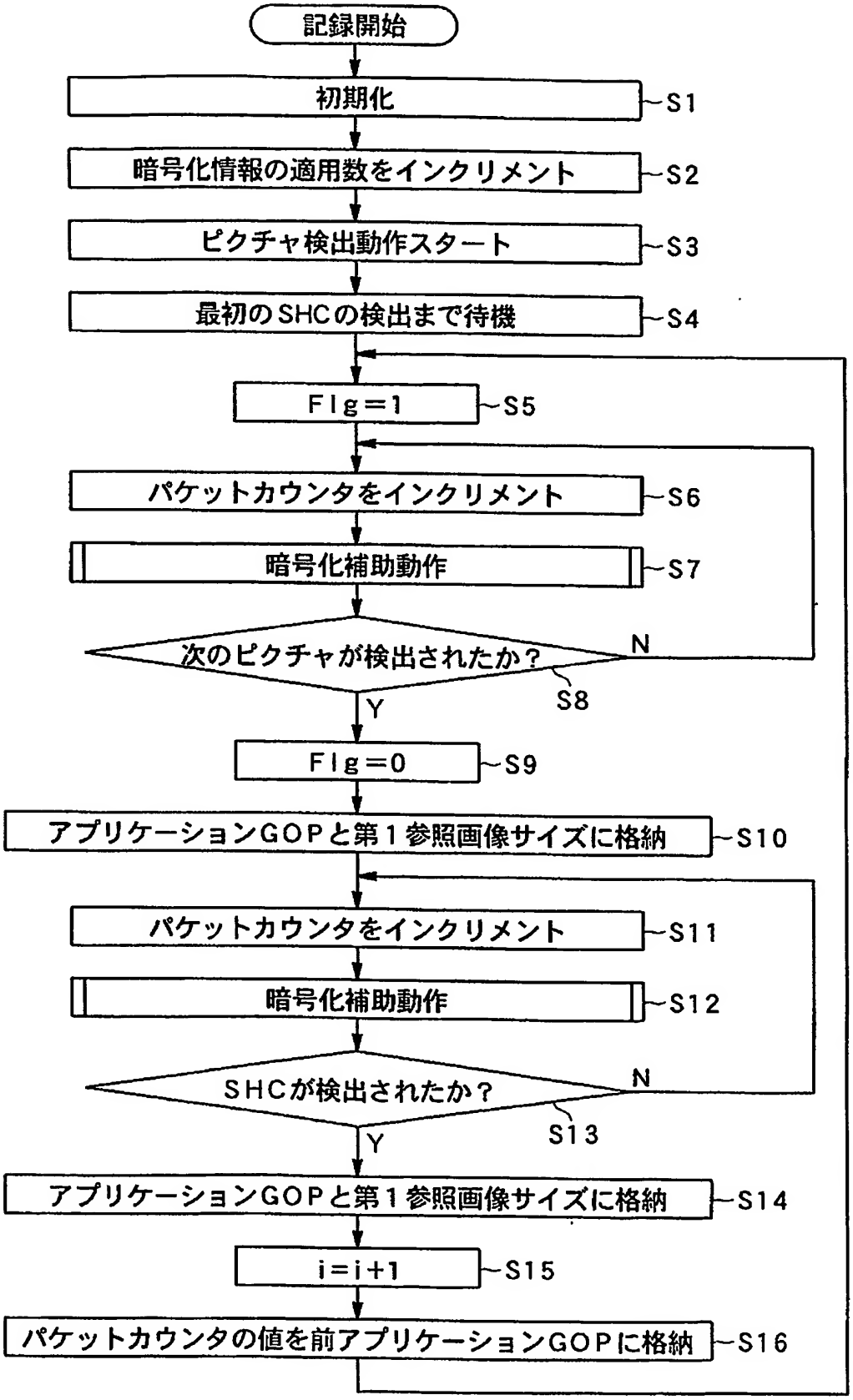
【図３】


TV
映像
音声L,R
20
22
映像音声
データデコーダ
26
メモリ
25
CPU
28
24
レコード
モジュール
パーシャルTS
27
IDEコントローラ
1
HDD
21
デマルチプレクサ
23
プレイバック
モジュール
MPEG-TS

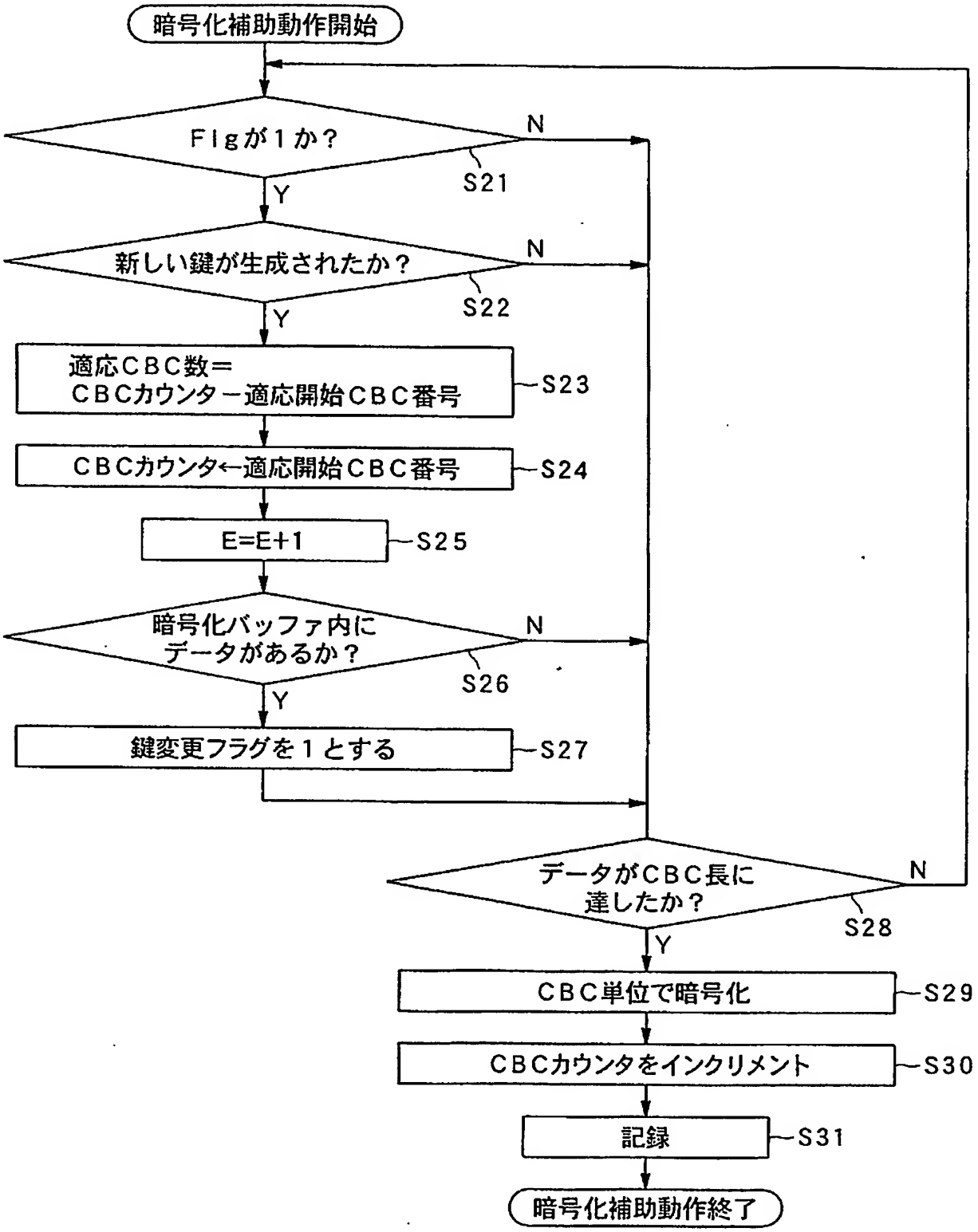
【図４】


24
32
31
情報化部
情報供給部
CBCカウンタ
パーシャルTS
特定単位情報
識別状態
フラグ
暗号化ストリーム
31a
32a
パケット
カウンタ
31b

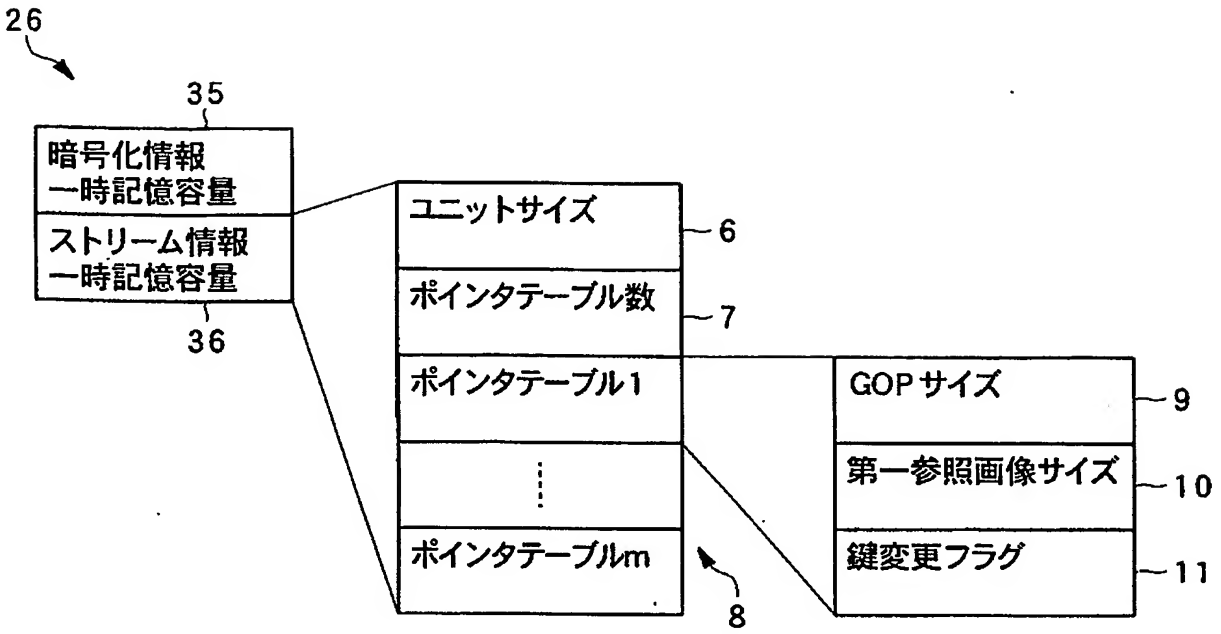
【図５】


記録開始
初期化
S1
暗号化情報の適用数をインクリメント
S2
ピクチャ検出動作スタート
S3
最初のSHCの検出まで待機
S4
Flg＝1
S5
パケットカウンタをインクリメント
S6
暗号化補助動作
S7
次のピクチャが検出されたか？
N
S8
Y
Flg＝0
S9
アプリケーションGOPと第１参照画像サイズに格納
S10
パケットカウンタをインクリメント
S11
暗号化補助動作
S12
SHCが検出されたか？
N
S13
Y
アプリケーションGOPと第１参照画像サイズに格納
S14
i＝i＋1
S15
パケットカウンタの値を前アプリケーションGOPに格納
S16

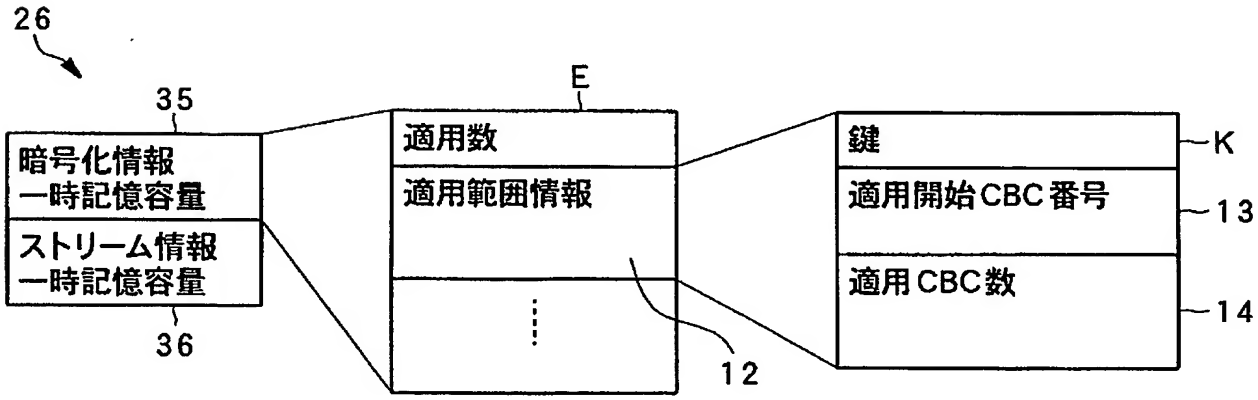
【図６】


暗号化補助動作開始
Ｆｌｇが１か？
N
S21
Y
新しい鍵が生成されたか？
N
S22
Y
適応ＣＢＣ数＝
ＣＢＣカウンター適応開始ＣＢＣ番号
S23
ＣＢＣカウンタ←適応開始ＣＢＣ番号
S24
E=E+1
S25
暗号化バッファ内に
データがあるか？
N
S26
Y
鍵変更フラグを１とする
S27
データがＣＢＣ長に
達したか？
N
S28
Y
ＣＢＣ単位で暗号化
S29
ＣＢＣカウンタをインクリメント
S30
記録
S31
暗号化補助動作終了

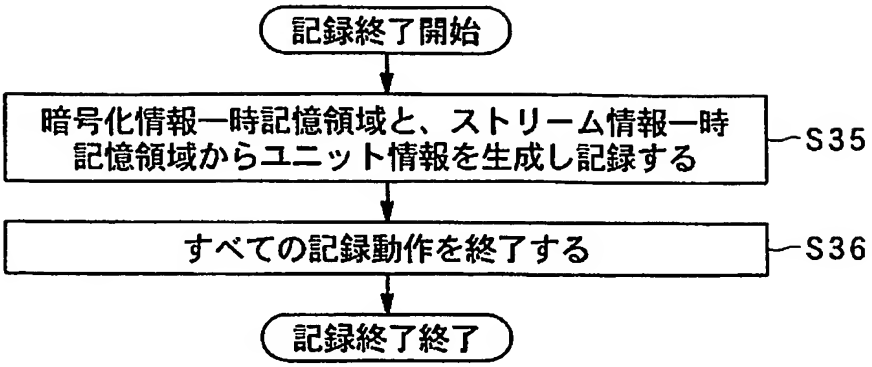
【図７】


26
35
暗号化情報
一時記憶容量
ストリーム情報
一時記憶容量
36
ユニットサイズ
6
ポインタテーブル数
7
ポインタテーブル1
ポインタテーブルm
8
GOPサイズ
9
第一参照画像サイズ
10
鍵変更フラグ
11

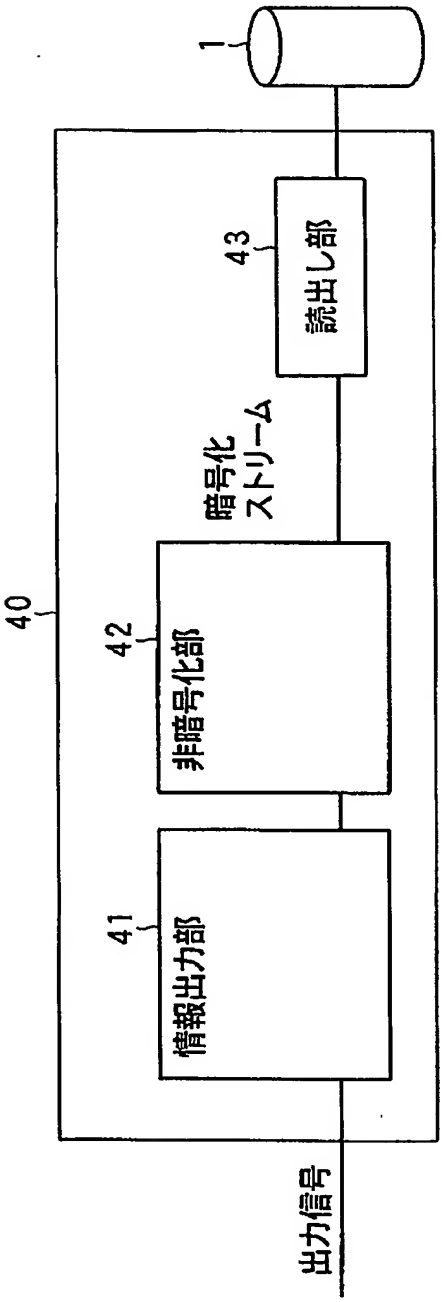
【図８】


26
35
暗号化情報
一時記憶容量
ストリーム情報
一時記憶容量
36
E
適用数
適用範囲情報
12
鍵
K
適用開始CBC番号
13
適用CBC数
14

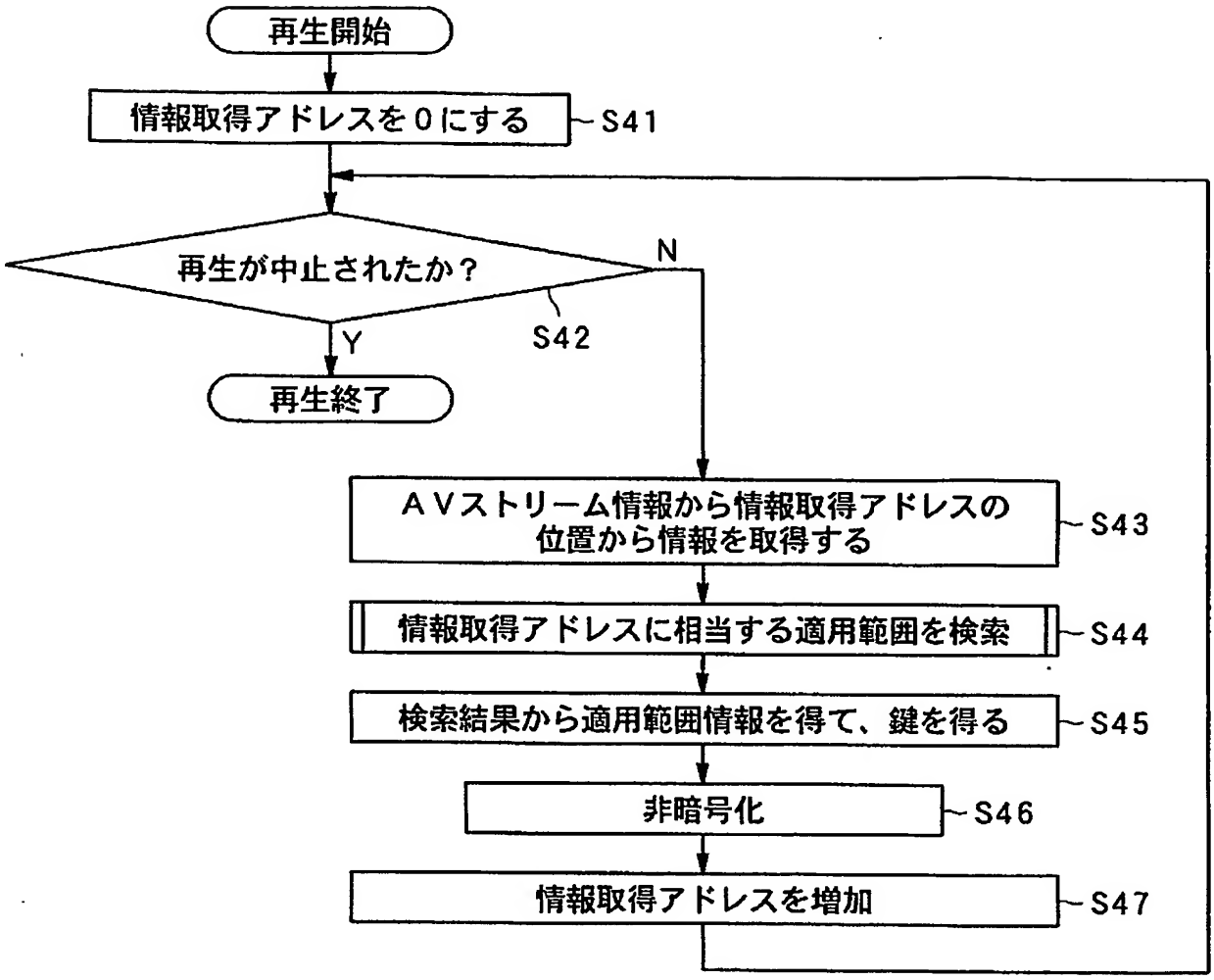
【図９】


記録終了開始
暗号化情報一時記憶領域と、ストリーム情報一時記憶領域からユニット情報を生成し記録する
S35
すべての記録動作を終了する
S36
記録終了終了

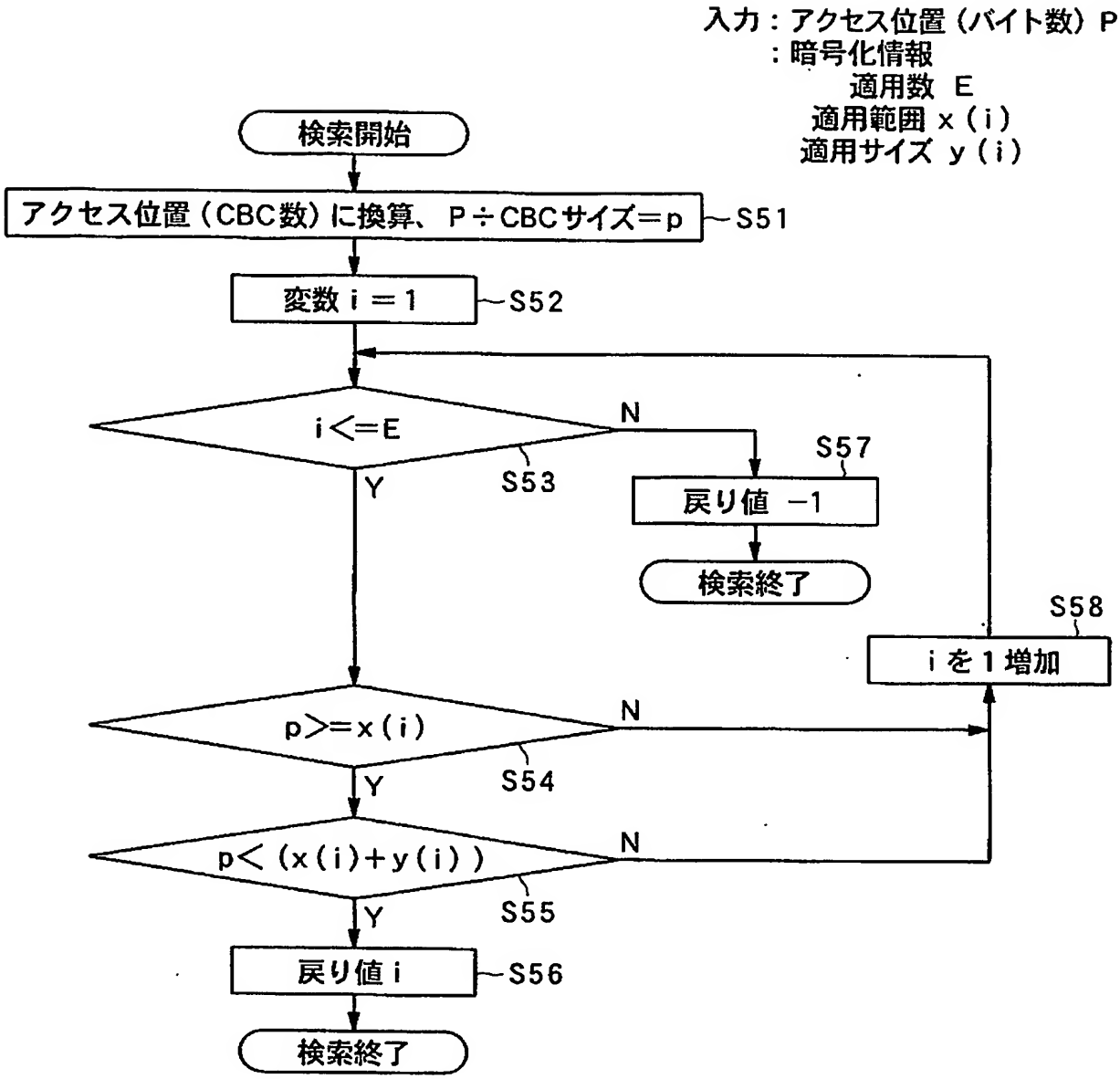
【図１０】



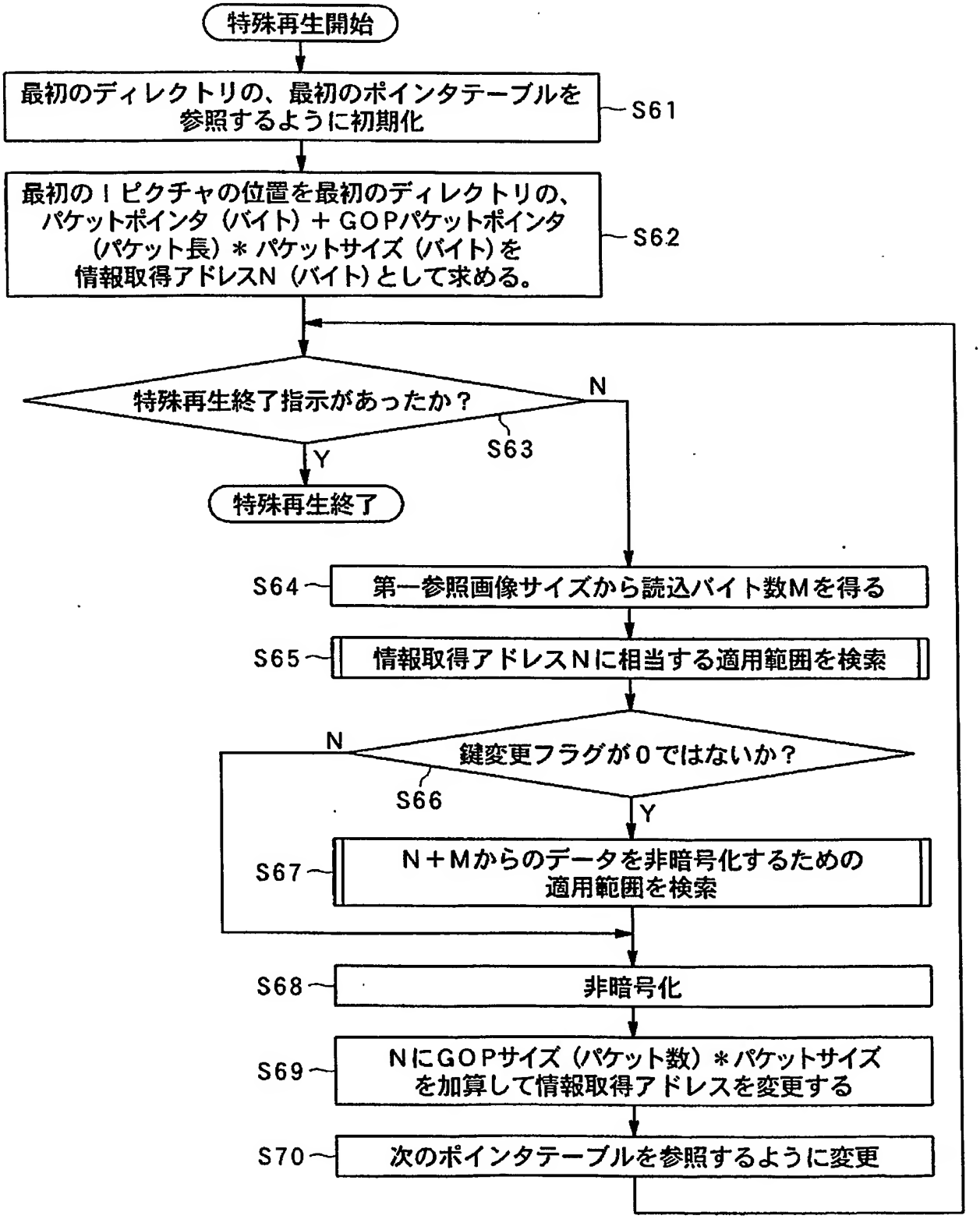
【図１１】


再生開始
情報取得アドレスを０にする
S41
再生が中止されたか？
N
Y
S42
再生終了
ＡＶストリーム情報から情報取得アドレスの位置から情報を取得する
S43
情報取得アドレスに相当する適用範囲を検索
S44
検索結果から適用範囲情報を得て、鍵を得る
S45
非暗号化
S46
情報取得アドレスを増加
S47

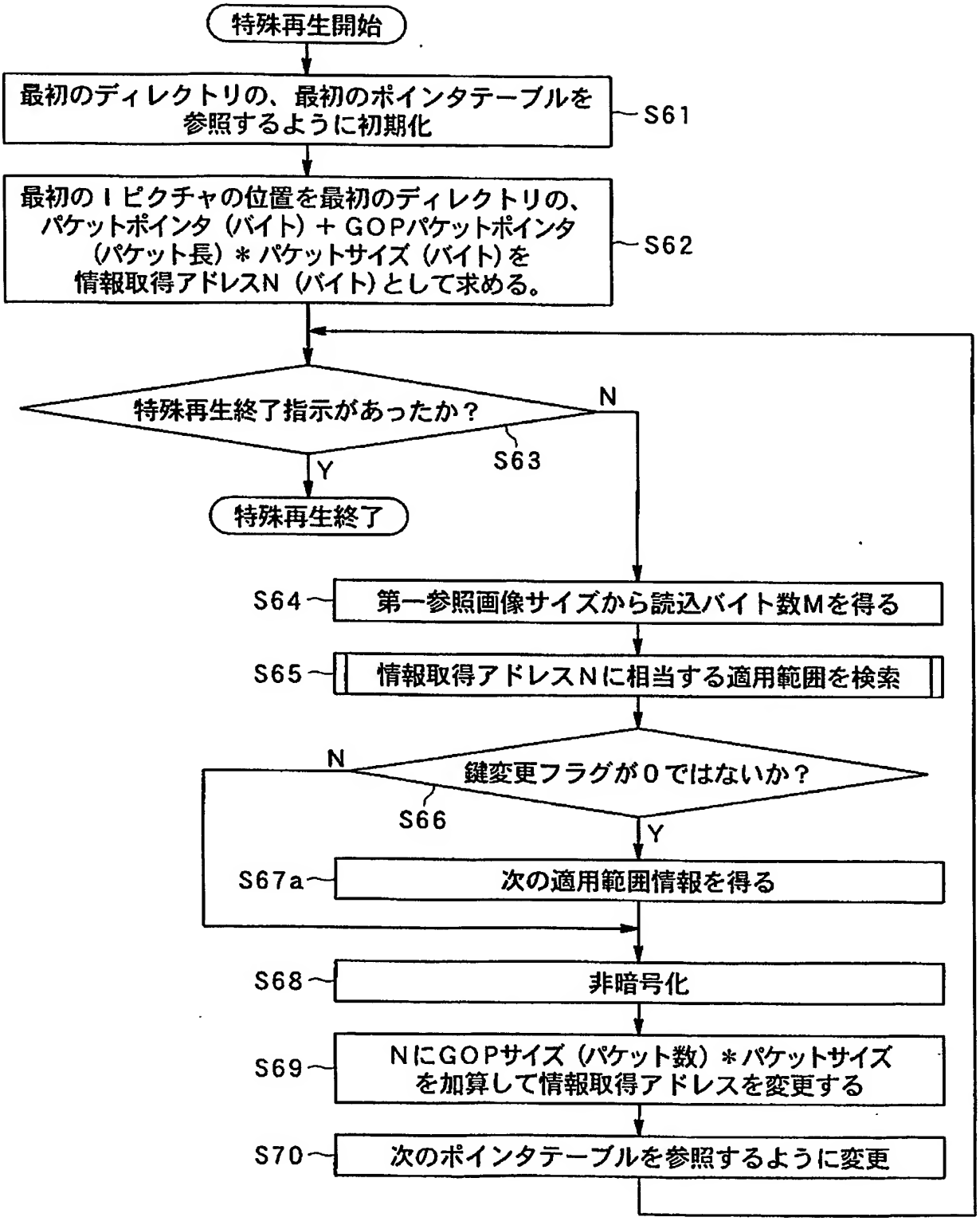
【図１２】


入力：アクセス位置（バイト数）P
：暗号化情報
適用数 E
適用範囲 x（i）
適用サイズ y（i）
検索開始
アクセス位置（CBC数）に換算、P÷CBCサイズ＝p
S51
変数 i ＝1
S52
i<=E
N
S53
Y
S57
戻り値 −1
検索終了
S58
i を１増加
p>=x(i)
N
S54
Y
p< (x(i)+y(i))
N
S55
Y
戻り値 i
S56
検索終了

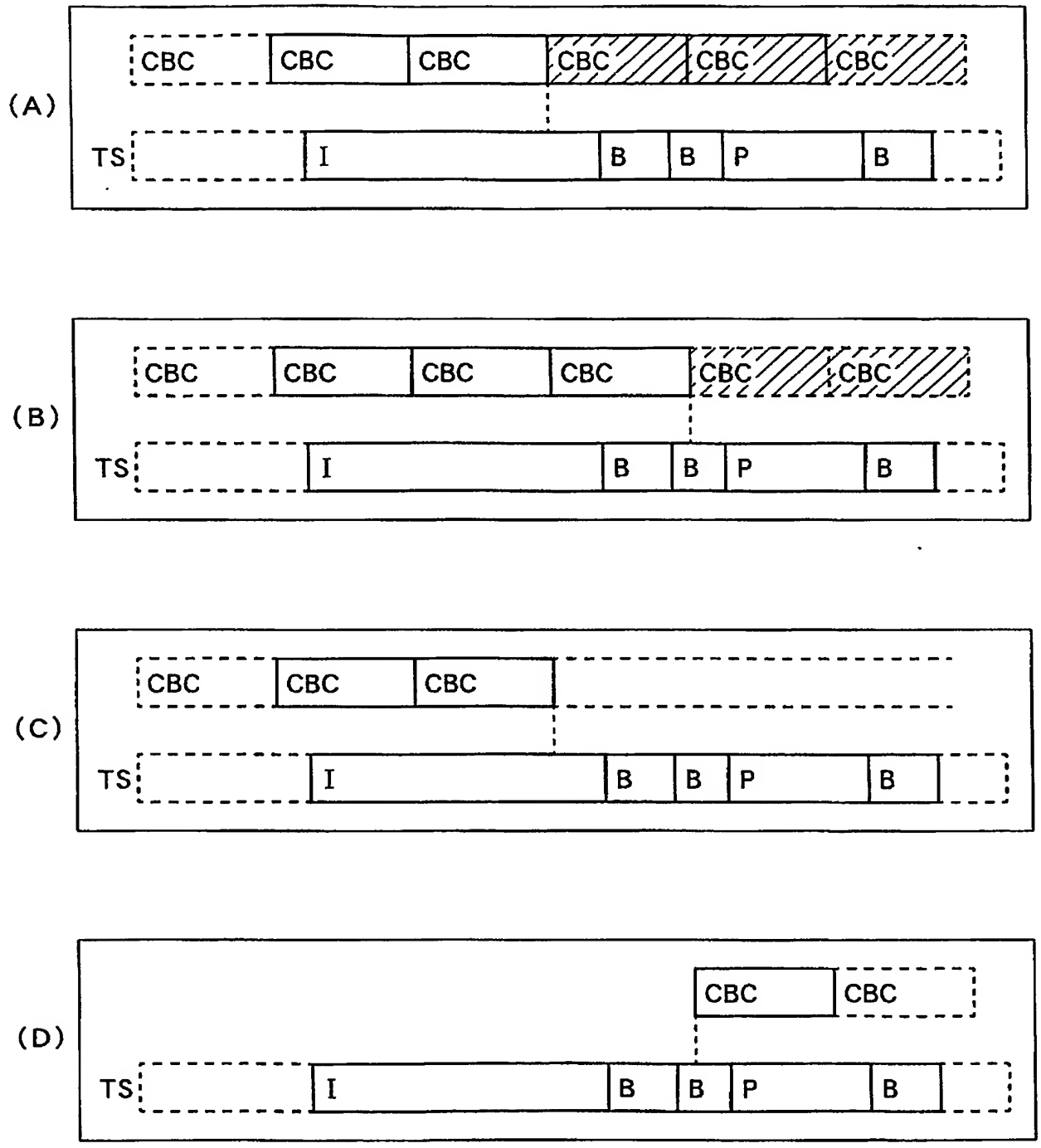
【図１３】


特殊再生開始
最初のディレクトリの、最初のポインタテーブルを参照するように初期化
S61
最初のＩピクチャの位置を最初のディレクトリの、パケットポインタ（バイト）＋ＧＯＰパケットポインタ（パケット長）＊パケットサイズ（バイト）を情報取得アドレスＮ（バイト）として求める。
S62
特殊再生終了指示があったか？
N
Y
S63
特殊再生終了
S64
第一参照画像サイズから読込バイト数Ｍを得る
S65
情報取得アドレスＮに相当する適用範囲を検索
鍵変更フラグが０ではないか？
N
Y
S66
S67
Ｎ＋Ｍからのデータを非暗号化するための適用範囲を検索
S68
非暗号化
S69
ＮにＧＯＰサイズ（パケット数）＊パケットサイズを加算して情報取得アドレスを変更する
S70
次のポインタテーブルを参照するように変更

【図１４】


特殊再生開始
最初のディレクトリの、最初のポインタテーブルを参照するように初期化
S61
最初のＩピクチャの位置を最初のディレクトリの、パケットポインタ（バイト）＋GOPパケットポインタ（パケット長）＊パケットサイズ（バイト）を情報取得アドレスN（バイト）として求める。
S62
特殊再生終了指示があったか？
N
S63
Y
特殊再生終了
S64
第一参照画像サイズから読込バイト数Mを得る
S65
情報取得アドレスNに相当する適用範囲を検索
N
鍵変更フラグが０ではないか？
S66
Y
S67a
次の適用範囲情報を得る
S68
非暗号化
S69
NにGOPサイズ（パケット数）＊パケットサイズを加算して情報取得アドレスを変更する
S70
次のポインタテーブルを参照するように変更

【図１５】


(A)
CBC
CBC
CBC
CBC
CBC
CBC
TS
I
B
B
P
B
(B)
CBC
CBC
CBC
CBC
CBC
CBC
TS
I
B
B
P
B
(C)
CBC
CBC
CBC
TS
I
B
B
P
B
(D)
CBC
CBC
TS
I
B
B
P
B

【書類名】要約書
【要約】
【課題】　暗号鍵の適用切り替わり時点を逐一算出する必要をなくし、円滑な処理を実行可能な情報記録媒体を提供すること。
【解決手段】　ハードディスク１には、アプリケーションＧＯＰにより構成されるＭＰＥＧ２規格におけるトランスポートストリームを、当該アプリケーションＧＯＰと異なるＣＢＣブロックの境界において暗号鍵を変更しつつ暗号化して得られた暗号化情報が記録されているＡＶストリーム情報３と、上記暗号化情報におけるアプリケーションＧＯＰに含まれるＩピクチャの解読に複数の暗号鍵が必要か否かを示す鍵変更情報が記録されている鍵変更フラグ１１と、が記録されている。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３７３０９７
受付番号	５０３０１８１４４４７
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年１１月　４日

＜認定情報・付加情報＞

【提出日】　平成15年10月31日

出願人履歴情報

識別番号　[０００００５０１６]

１．変更年月日　１９９０年　８月３１日
[変更理由]　新規登録
住　所　東京都目黒区目黒１丁目４番１号
氏　名　パイオニア株式会社